

Analisis Tingkat Keamanan Enkripsi Data Menggunakan Algoritma Base 64 Endcode

Annas Apreja¹

Sistem Informasi Professional
Fakultas Ilmu Komputer
Universitas Sriwijaya
annasapreja95@gmail.com

Zulfadhli Syarif²

Sistem Informasi Professional
Fakultas Ilmu Komputer
Universitas Sriwijaya
zulfadlysyarif12@gmail.com

Ali Ibrahim³

Dosen Sistem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
aliibrahim@ilkom.unsri.ac.id

Abstrak - Di era digital seperti sekarang ini sistem informasi semakin berkembang. Sebagai indikator dapat dilihat dari kemajuan teknologi dalam pengamanan data yang semakin lama semakin berkembang seiring dengan kebutuhan manusia dengan komunikasi data. Analisis keamanan data menggunakan Algoritma Base64 merupakan suatu analisa tentang bagaimana tingkat keamanan algoritma ini yang familiar digunakan oleh pengembang. Semakin berkembangnya pengetahuan, dikembangkan pula algoritma Base64. Base64 adalah metode yang digunakan untuk melakukan penyandian terhadap data biner menjadi teks, data biner disandikan menjadi format 7-bit character. Dengan adanya analisa ini kita bisa mengetahui tingkat keamanan dari data dengan menggunakan algoritma Base64.

Kata kunci : *base64, algoritma, data biner*

I. PENDAHULUAN

Data merupakan salah satu asset penting dalam kelangsungan hidup perusahaan manapun, instansi pemerintah maupun instansi pendidikan penyimpanan data memerlukan berbagai macam pertimbangan terutama dari segi keamanan dan kerahasiannya.

Pengaman data merupakan salah satu aspek untuk menyelamatkan data-data dari kemungkinan terjadinya pencurian dan pengubahan data oleh pihak yang tidak dikenal. Peningkatan kerahasiaan data dari waktu ke waktu mengalami banyak perubahan, di antaranya dengan menggunakan metode kriptografi. Algoritma penyandian yang dikenal dengan kriptografi telah mencakup aspek kehidupan manusia saat ini. Begitu pentingnya kriptografi, saat berbicara tentang keamanan data, orang tidak bisa memisalkannya dengan kriptografi[1]

Di dalam kriptografi terdapat metode enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi atau data dengan membuat informasi atau data tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus, sebaliknya dekripsi merupakan proses pengembalian informasi atau data yang sebelumnya telah di enkripsi supaya dapat dibaca kembali.

Dari beberapa metode yang ada di dalam enkripsi dan dekripsi, adalah base64 yang merupakan metode yang digunakan untuk melakukan penyandian terhadap data biner sehingga menjadi format teks atau menjadi format karakter 7-bit.

II. METODOLOGI PENELITIAN

Metode penelitian yang dilakukan terdiri dari: (1) Studi literatur, merupakan tahap pendalaman materi, identifikasi permasalahan dan teori yang berkaitan dengan permasalahan dalam penelitian. (2) Pengumpulan data, bertujuan untuk mendapatkan data teks yang akan digunakan sebagai masukan dari sistem. (3) Analisa performansi, bertujuan untuk melakukan analisa performansi dari skema enkripsi dan dekripsi dengan menggunakan Base64 Encode. (4) Pengambilan kesimpulan, bertujuan untuk menarik kesimpulan setelah melakukan penelitian tentang Base64 Encode.

III. IDENTIFIKASI MASALAH

Saat ini kriptografi memegang peran penting dalam keamanan data di seluruh dunia. Saat ini sudah banyak metode-metode yang dilakukan dalam seni kriptografi. Pada algoritma base64 pesan akan di enkripsi *Encoding* dan *Decoding* ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan encoding (penyandian) terhadap data binary[2].

Tabel 1 Encoding Base64 [2]

Data 6 bit	Karakter encoding 64	Data 6 bit	Karakter encoding 64	Data 6 bit	Karakter encoding 64	Data 6 bit	Karakter encoding 64
0	A	16	Q	32	h	48	y
1	B	17	R	33	i	49	z
2	C	18	S	34	j	50	0
3	D	19	T	35	k	51	1
4	E	20	U	36	l	52	2
5	F	21	V	37	m	53	3
6	G	22	W	38	n	54	4
7	H	23	X	39	o	55	5
8	I	24	Y	40	p	56	6
9	J	25	Z	41	q	57	7
10	K	26	a	42	r	58	8
11	L	27	b	43	s	59	9
12	M	28	c	44	t	60	+
13	N	29	d	45	u	61	/
14	O	30	e	46	v	62	=
15	P	31	f	47	w	pad	
16	Q	32	g	48	x		

Keamanan algoritma base64 terdapat pada indexnya, dimana plainteks yang dimasukan akan diproses dan dikonversi kedalam tabel index berdasarkan tabel 1[2]. Tingkat keamanan algoritma base64 sudah cukup tinggi karena melewati beberapa proses pemecahan bit huruf atau angka pesan asli. Berikut adalah proses pendekripsian algoritma base64 [3]:

- Pecah *string byets* tersebut ke per 3 bytes

- b. Menggabungkan 3 byets menjadi 24bit, 1bytes = 8 bit, $3 \times 8 = 24\text{bit}$. 2012, no. Snati, pp. 47–52, 2012.
- c. 24bit dipecah menjadi 6 bit, sehingga menjadi 4 pecahan
- d. Pecahan diubah kedalam bilangan desimal, dengan nilai maksimal 6 bit adalah 63
- e. Menjadikan nilai desimal tersebut menjadi indeks untuk memilih karakter penyusun dari base64.

Contoh kasus :

Bilangan asli : E

ASCII : 69

Bit : 01000101

Index : 16 17

Base64 : R Q ==

Diagram algoritma base 64

Kelemahan base64 endcode karena dalam salah satu pemrograman yaitu PHP sudah memiliki coding untuk decode base64, sehingga tingkat keamanan dari base64 turun, jika tidak di kombinasikan dengan algoritma lainnya.

IV. HASIL DAN BAHASAN

Setelah melakukan penelitian dan analisa dari proses enkripsi algoritma base64, tingkat keamanan dari base 64 sudah cukup tinggi, karena harus melewati proses mengubah kebilangan binery dan menjadikan nya ke sebuah index stelah bit dipecah. Namun yang menjadi kelemahan enkripsi base64, sudah ada dibuatnya suatu fungsi pada bahasa pemrograman php untuk mendecode enkripsi dari base64 dengan mudah.

V. KESIMPULAN

Ada beberapa kesimpulan yang diambil:

- a. Tingkat keamanan sistem jika hanya menggunakan dan mengandalkan enkripsi base64 maka tingkat kemaanan sistem akan sangat lemah.
- b. Pengkombinasian algoritma akan sangat meningkatkan suatu sistem, agar para hacker harus berkerja lebih sulit untuk mendeskripsikan suatu data yang dienkrpsi double

VI. DAFTAR PUSTAKA

- [1] A. Zelvina, S. Efendi, D. Arisandi, and U. S. Utara, "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa," vol. 1, no. 1, pp. 56–62, 2012.
- [2] A. T. SHOLEH, E. GUNADHI, and A. D. SUPRIATNA, "Mengamankan Skrip Pada Bahasa Pemograman Php Dengan Menggunakan Kriptografi Base64," *J. Algoritm. Sekol. Tinggi Teknol. Garut*, vol. 10, no. 1, pp. 1–9, 2013.
- [3] F. W. C, A. P. Rahagiari, and F. Fretes, "Penerapan Algoritma Gabungan Rc4 Dan Base64 Pada Sistem Keamanan E-Commerce," *Semin. Nas. Apl. Teknol. Inf.*, vol.